INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 3, Numărul 2, Iunie 2024

Provocarea globală de război electronic în 2024: Principalii jucători

Nicolae Sfetcu

Sfetcu, Nicolae (2024), Provocarea globală de război electronic în 2024: Principalii jucători, *Intelligence Info*, **3**:2, 3-18, DOI: 10.58679/II50473, https://www.intelligenceinfo.org/provocarea-globala-de-razboi-electronic-in-2024-principalii-jucatori/

Publicat online: 23.04.2024

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Provocarea globală de război electronic în 2024: Principalii jucători

Ing. fiz. Nicolae SFETCU, MPhil[1]
nicolae@sfetcu.com

The Global Electronic Warfare Challenge in 2024: The Major Players

Abstract

Geopolitical tensions and regional conflicts have intensified the race for electronic warfare supremacy. Nations perceive EW capabilities as force multipliers, providing strategic advantages in contested regions and deterring potential adversaries. The development and deployment of EW technologies are closely related to broader strategic goals that reflect each entity's geopolitical goals and concerns.
This essay analyzes the dynamics of international competition in advanced electronic warfare by examining the main players in this evolving geopolitical arena.
Keywords: electronic warfare, electromagnetic warfare, USA, China, Russia, NATO, European Union

Rezumat

Tensiunile geopolitice și conflictele regionale au intensificat cursa pentru supremația războiului electronic. Națiunile percep capacitățile EW ca multiplicatori de forță, oferind avantaje strategice în regiunile contestate și descurajând potențialii adversari. Dezvoltarea și implementarea tehnologiilor EW sunt strâns legate de obiective strategice mai largi, care reflectă obiectivele și preocupările geopolitice ale fiecărei entități.
Acest eseu analizează dinamica competiției internaționale în războiul electronic avansat, examinând principalii jucători în această arenă geopolitică în evoluție.
Cuvinte cheie: războiul electronic, război electromagnetic, SUA, China, Rusia, NATO, Uniunea Europeană

INTELLIGENCE INFO, Volumul 3, Numărul 2, Iunie 2024, pp. 3-18
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II50473
URL: https://www.intelligenceinfo.org/provocarea-globala-de-razboi-electronic-in-2024-principalii-jucatori/
© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

Articol în Acces Deschis (Open Access) distribuit în conformitate cu termenii licenței de atribuire Creative Commons CC BY SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0/)

Introducere

Războiul electronic (EW) a apărut ca o arenă critică pentru competiția globală. Națiunile din întreaga lume luptă pentru superioritate în acest domeniu, recunoscând rolul său esențial în războiul modern și securitatea națională. Capacitățile avansate de război electronic cuprind un spectru de tehnologii și tactici, inclusiv contramăsuri electronice, informații despre semnal și război cibernetic.

Tensiunile geopolitice și conflictele regionale au intensificat cursa pentru supremația războiului electronic. Națiunile percep capacitățile EW ca multiplicatori de forță, oferind avantaje strategice în regiunile contestate și descurajând potențialii adversari.

Dependența din ce în ce mai mare de sistemele digitale interconectate expune națiunile la vulnerabilități cibernetice, subminând rezistența capacităților lor de război electronic. Atacurile cibernetice sofisticate pot perturba operațiunile EW, pot compromite informații sensibile și pot eroda avantajul strategic.

Intensificarea competiției internaționale în războiul electronic ridică îngrijorări cu privire la riscul de escaladare și a consecințelor neintenționate. Interpretarea greșită a activităților EW, interferența involuntară sau calculele greșite ar putea escalada tensiunile, ducând la escaladarea accidentală a conflictelor sau la provocări de control.

Competitorii principali identificați de SUA în Strategia Națională de Apărare din 2022 sunt China și Rusia. Aceștia, observând că întreruperea sistemelor C&C ar putea fi o soluție rentabilă pentru diminuarea avantajelor militare ale SUA[2], s-au concentrat pe dezvoltarea de sisteme EW, pentru o dominație informațională[3].

SUA

SUA au o abordare de lungă durată și sofisticată a EW, punând accent atât pe capacitățile ofensive, cât și pe cele defensive. Aceasta implică utilizarea mijloacelor electronice pentru a controla spectrul electromagnetic (EMS) și pentru a ataca sau apăra

[2] (Hoehn 2021)
[3] (Copp 2021)

împotriva activelor inamice din acel spectru. Armata SUA integrează EW în toate ramurile, folosind adesea tehnologii avansate, cum ar fi activitățile ciber-electronice (CEMA) și dezvoltând noi instrumente, cum ar fi Sistemul Integrat de Augmentare Vizuală (IVAS).

Războiul electronic (EW), este definit de Departamentul Apărării SUA (DoD) ca ”activități militare care folosesc energia electromagnetică pentru a controla spectrul electromagnetic („spectrul”) și pentru a ataca un inamic”[4].

Strategia națională de apărare a SUA, lansată în 2022, evidențiază eforturile Chinei și Rusiei de a-și moderniza forțele pentru a contracara avantajele militare ale SUA. Comisia pentru Strategia Națională de Apărare a declarat că Statele Unite își pierd avantajele în războiul electronic, recomandând creșterea investițiilor EW și dezvoltarea de noi concepte. Armata intenționează să investească atât în programe de EW la bord, cât și la sol, prin achiziționarea de sisteme EW de rezistență lungă, fără pilot aerian și instruire la nivel de unitate. Marina continuă să susțină și să-și modernizeze batalioanele radio concepute pentru informații despre semnături și război electronic, dezvoltă conceptul Naval Integrated Fire Control-Counter Air (NIFC-CA) pentru a ajuta aerian să contracareze adversarii în medii imposibile sau degradate, și finanțează proiectul Next Generation Jammer[5].

Comitetul Executiv al EW din cadrul DOD, condus de secretarul adjunct al Apărării, are sarcina de a ”sincroniza și integra EW între componentele DOD prin partajarea tacticilor, tehnicilor, procedurilor și tehnologiilor”[6] și de a stabili politica DOD pentru EW. Actul de autorizare a apărării naționale FY2019 a inclus crearea unei echipe interfuncționale pentru operațiunile cu spectrul electromagnetic. Strategia de superioritate a spectrului electromagnetic a fost publicată pe 29 octombrie 2020.

Conceptul operațional de comandă și control comun al tuturor domeniilor din Statele Unite (JADC2) urmărește să „simtă”, „să înțeleagă” și să „acționeze” rapid asupra informațiilor din spațiul de luptă prin utilizarea automatizării, inteligenței artificiale, analizei predictive și învățării automate (ML)[7]. Perspectiva SUA, axată pe optimizarea

[4] (CRS 2022)
[5] (CRS 2022)
[6] (CRS 2022)
[7] (DoD 2022)

operațiunilor, neglijează accentul suplimentar pe sisteme contradictorii. EW este condiția esențială a implementării cu succes a JADC2.

Prin combinarea mecanismelor EW cu operațiunile MILDEC 44, SUA pot crea haos pentru sistemele adverse prin injectarea unor cantități copleșitoare de semnale și date, dar cu riscul de a crea un haos suplimentar pentru forțele prietene. Dar se consideră că haosul controlat este soluția pentru a înșela amenințările de înaltă fidelitate, avansate și emergente[8].

Instrumentul de planificare și management al războiului electronic al armatei (EWPMT) permite unui comandant să înțeleagă și să vizualizeze mai bine spectrul electromagnetic de pe câmpul de luptă în timpul unei operațiuni[9].

Armata a dezvoltat două sisteme numite Terrestrial Layer Systems, care vor furniza război electronic integrat și capabilități cibernetice pe câmpul de luptă.

Programul TLS-Brigade Combat Team va oferi soldaților capacități integrate de război electronic, cibernetic și informații de semnale la nivel de brigadă.

În 2021, Northrop Grumman Corporation a livrat unul dintre cei mai avansați senzori multifuncționali, Arrays at Commercial Timescales-Integration and Validation (ACT-IV), care se bazează pe o matrice avansată multifuncțională digitală activă scanată electronic (AESA).

Prin programul Multi-Function Electronic Warfare-Air Large (MFEW-AL), Armata SUA pregătește operațiuni multi-domeniu și ia în considerare distanțele mari din Pacific.

Armata urmează să acorde o atenție deosbită războiului electronic și roiurilor de drone, prin EDGE 22. Armata intenționează, de asemenea, să experimenteze cu capacități de detectare multi-intelligence.

SEWIP este programul general al Marinei pentru a încorpora diverse capacități EW în navele sale, folosind versiuni de SLQ-32, capacitatea asociată cu SEWIP[10].

{9} Acțiuni în cadrul unui potențial EW[11]:

[8] (Duke 2023)
[9] (Northrop 2022)
[10] (Northrop 2022)
[11] (Army 2020)

- *Organizarea pentru război electronic* comun: Planificarea și operațiunile EW pot fi împărțite între mai multe direcții ale unui personal comun; statul major EW al comandantului forței comune de război electronic comun (JCEWS) este condus de un ofițer de comandă a războiului electronic. JCEWS dezvoltă planuri de operare (OPLAN) și planuri conceptuale și monitorizează operațiunile și activitățile EW de rutină.
- *Organizația de asistență de informații pentru războiul electronic*: Fiecare comandant la nivel geografic trebuie să stabilească o structură de gestionare a frecvenței care să includă un birou comun de gestionare a frecvenței (JFMO) și să stabilească proceduri pentru a sprijini operațiunile planificate și în curs. Armata este organizată să lucreze în structura unui grup de lucru de război electronic cu întemeierea grupului centrat pe EWO, tehnicianul EW și specialistul EW, care cuprind celula de coordonare a războiului electronic (EWCC). Activele marine EW sunt parte integrantă a grupului operativ maritim aer-sol (MAGTF).
- *Aspecte multinaționale ale războiului electronic:* Planificatorii din SUA ar trebui să integreze capacitățile EW ale SUA și ale țărilor partenere într-un plan general EW, oferind națiunilor partenere informații despre capabilitățile EW ale SUA și asistență EW națiunilor partenere.

Securitatea națională a Statelor Unite este acum dependentă de marile companii de tehnologie, care au o influență puternică asupra factorilor de decizie politică[12]. Acestea au cei mai talentați oameni și dețin drepturile asupra celor mai puternice arme[13].

China

China a investit în mod semnificativ în războiul electronic ca parte a strategiei sale militare moderne, concentrându-se în mare măsură pe a ajunge lider mondial în ceea ce ei numesc „război informațional”. Aceasta include dezvoltarea capacităților de a perturba sistemele de comunicații și navigație ale potențialilor adversari. Strategia Chinei implică integrarea războiului electronic în toate nivelurile operațiunilor lor militare, subliniind importanța războiului cibernetic, a spionajului electronic și a altor forme de conflict digital ca o completare a angajamentelor militare tradiționale.

În 2021, China a făcut public un nou concept operațional numit Multidomain Precision Warfare (Război de precizie multidomeniu)[14], ca răspuns la JADC2. Deși este similar cu strategia SUA, acesta pune mai mult accent pe identificarea vulnerabilităților

[12] (Henney 2019)
[13] (Kolhatkar 2019)
[14] (Insinna 2022)

adversarilor prin intermediul AI prin măsuri cinetice și non-cinetice. China pune accent pe vizarea vulnerabilităților tehnologiilor emergente ale SUA.

Strategia AI a Chinei a fost acoperită de Elsa Kania, un coleg senior adjunct pentru tehnologie și securitate națională la Centrul pentru o nouă securitate americană. „China nu a făcut niciun secret al obiectivului său de a conduce lumea în AI, iar militarii, în special, a înregistrat un progres mai mare decât se aștepta. Aceasta include o listă lungă de aplicații, cum ar fi drone sinucigașe, sisteme de arme autonome, EW, operații cibernetice, Wargaming, Analytics Data și Conștientizare situațională", a spus ea[15].

În iulie 2017, Consiliul de Stat al Chinei a lansat un plan și o strategie de inteligență artificială prin care să devină liderul mondial în domeniul inteligenței artificiale până în 2030, angajând 150 de miliarde de dolari pentru acest obiectiv[16]. La finele anului 2019 China își atinsese obiectivul mai devreme decât se aștepta[17]. Un avantaj al strategiei a Chinei a fost dezvoltarea de noi sisteme inovatoare[18]. Astfel, China posedă sofisticarea și resursele de a pirata sistemele de rețea, de a stabili puncte de sprijin în spatele apărării perimetrale, de a filtra informații valoroase și de a sabota funcțiile critice ale rețelei[19]. Din 2019, China este liderul mondial în tehnologia rachetelor cu dezvoltarea sistemelor de control de învățare cu întărire profundă pentru țintire și ghidare[2021].

Producătorii chinezi de arme vând deja drone înarmate controlate AI[22], companiile chineze care dezvoltă AI lucrând în cooperare cu armata chineză. De remarcat că dezvoltarea, de către China de arme robotizate din ce în ce mai autonome și tehnologia IA de supraveghere contravine obiectivelor declarate ale Chinei de a evita o cursă a înarmărilor AI[23].

[15] (Friedrich 2020)
[16] (Baker 2018)
[17] (Allen 2019)
[18] (Rogosa 2015)
[19] (Carlin 2016)
[20] (You, Diao, și Gao 2019)
[21] (Haney 2019)
[22] (Allen 2019)
[23] (Haney 2019)

Rusia

Capacitățile de război electronic ale Rusiei sunt unele dintre cele mai avansate din lume. Țara și-a demonstrat capacitățile EW în diferite conflicte, în special în Ucraina și Siria. Eforturile rusești EW se concentrează pe perturbarea comunicațiilor și a senzorilor inamicului, orbindu-i și derutând astfel adversarii. Desfășurarea unor astfel de tehnologii a fost cheia strategiei Rusiei de război hibrid, în care operațiunile militare convenționale sunt combinate cu metode mai ascunse sau netradiționale de conflict, inclusiv atacuri cibernetice și înșelăciune electronică.

În decembrie 2010, armata rusă a s-a dotat cu primul său sistem de război electronic multifuncțional (Borisoglebsk 2), montat pe nouă vehicule blindate MT-LB și folosit pentru a suprima comunicațiile mobile prin satelit și semnalele de navigație prin satelit[24].

Potrivit unui raport din 2017 al Centrului Internațional pentru Apărare și Securitate, portofoliul EW al Rusiei este orientat spre comunicațiile NATO, radarele, vehiculele aeriene fără pilot și alți senzori provocatori[25].

Potrivit lui Margarita Konaev, de la Centrul pentru Securitate și Tehnologie Emergentă, „Rusia urmărește China și SUA în toate valorile AI. Cu toate acestea, armata sa conduce eforturile țării de a ajunge la pas în zone cheie, majoritatea implicând aplicații militare. ” Konaev a enumerat trei dintre concentrările de investiții ale Rusiei: robotica militară și sistemele fără pilot, capacitățile de război electronic (EW) și războiul informațional. Observând ritmul rapid al țării când vine vorba de experimentare, ea a spus: „Ei sunt repede de testat și învață limitări în condiții operaționale[26]”

Conform lui Jonas Kjellen[27], echivalentul rusesc modern al EW a fost denumit, cronologic, drept Contramăsuri radio (Radioprotivodeistvie, RPD), Echipament de combatere radioelectronică a inamicului (Borba s radioelektronnymi sredstvami protivnika, BRESP), și Radioelektronnaia borba (REB) începând cu anii 1960[28]. Conform Enciclopediei Militare Sovietice din 1984, războiul electronic este un set de măsuri luate pentru identificarea și utilizarea ulterioară a suprimării radioelectronice asupra

[24] (ODIN 2023)
[25] (Northrop 2022)
[26] (Friedrich 2020)
[27] (Kjellén 2018)
[28] (Liubin 2009)

echipamentelor și sistemelor radioelectronice adverse și pentru a proteja echipamentele și sistemele radioelectronice ale propriilor forțe[29]. EW sovietic era împărțit în măsuri EW ofensive („suprimare radioelectronică", Radioelektronnoe podavlenie) și defensive: „suprimare radioelectronică" (protecție radioelectronică", Radioelektronnaia zashchita).

Din 1990, definiția EW a suferit unele modificări; războiul electronic este un ansamblu de măsuri și acțiuni — interconectate în timp și prin ținte și sarcini — luate de trupe (forțe) pentru a detecta echipamentele și sistemele radioelectronice inamice și pentru a asigura distrugerea lor ulterioară (folosind orice tip de armă), eliminarea (scoaterea din lupta) sau suprimarea radioelectronica, precum si protectia radioelectronica a echipamentelor si sistemelor radioelectronice proprii fortelor; [războiul electronic] este o funcție de sprijinire a luptei[30].

Conform unor documente mai noi[31], războiul electronic este un ansamblu de activități și acțiuni coordonate care cuprind atacul radioelectronic asupra obiectelor radioelectronice și tehnico-informaționale adverse, protecția radioelectronică a obiectelor radioelectronice și tehnico-informaționale, contramăsuri împotriva recunoașterii tehnice și măsurile de susținere a informațiilor radioelectronice. În nou definiție apar două noi zone, contramăsuri împotriva recunoașterii și informațiilor tehnice și măsurile de sprijin pentru informații radioelectronice. Astfel, componentele războiului electronic rus modern sunt:

1. Atacul electronic, cu includerea armelor distructive EW[32], folosind atacul funcțional, contramăsuri electronice, rachete antiradiații, și simulare și imitație electronică.
2. Protecția electronică, ca măsuri pentru a asigura funcționalitatea echipamentelor radioelectronice într-un mediu blocat[33], incluzând întărirea electronică (creșterea rezistenței electronice la diferite tipuri de radiații electromagnetice) și compatibilitatea electromagnetică pentru reducerea interferențelor dăunătoare.
3. Contramăsuri împotriva recunoașterii tehnice (protivodeistvie tekhnicheskim sredstvam razvedki, PD TSR) pentru protejarea împotriva recunoașterii străine[34].
4. Măsuri de sprijin pentru informații radioelectronice pentru sprijinul celor trei de mai sus, inclusiv prin control tehnic cuprinzător[35].

[29] (* * * 1984, 615)
[30] (* * * 1990, 357)
[31] (Guzenko și Moraresku 2017, 14–16)
[32] (Lakhin și Korobeinikov 2016)
[33] (Kolesov și Nasenkov 2015, 17)
[34] (Krylov, Larionova, și Nikitina 2017, 74)
[35] (Krylov, Larionova, și Nikitina 2017, 165)

Rolul EW este acum mult mai larg și introduce un set mai mare de mijloace, inclusiv utilizarea de rachete antiradiații, DEW și capacități cibernetice, EW contemporan rus posedând capacități nu numai de a suprima temporar sistemul electronic al unui adversar, ci și de a provoca daune permanente.

În 2002, președintele Vladimir Putin a semnat un document de politică și strategie pe termen lung al EW, Osnovy politiki Rossiiskoi Federatsii v oblasti razvitiia sistemy radioelektronnoi borby na period do 2010 goda i dalneishuiu perspektivu (Politicile fundamentale pentru dezvoltarea Federației Ruse și până la sistemul de război electronic până în 2010). În februarie 2012, acest document de strategie a fost reînnoit. fiind valabil „până în 2020 și după”[36]. Cele cinci direcții principale ale noului document de strategie sunt: îmbunătățirea controlului de stat asupra funcționării și dezvoltării EW; integrarea domeniului militar EW cu alte domenii pentru securitatea națională; exploatarea realizărilor în cercetare și dezvoltare pentru o nouă generație de sisteme EW; dezvoltarea în continuare a sistemului EW educațional și de cercetare științifică; și extinderea cooperării militaro-tehnice și creșterea potențialului de export al sistemelor EW[37][38]

Unii experți notează că armele rusești EW sunt superioare celor americane în mai multe privințe[39]. Se consideră că Rusia este atât de mult focalizată pe EW întrucât este o modalitate relativ ieftină de a diminua capacitățile unui adversar., într-un efort de ”a contesta în mod asimetric statele membre [NATO] mai vulnerabile de la periferia alianței și de a maximiza șansele de succes într-o operațiune împotriva membrilor NATO din est înainte ca alianța să poată organiza un răspuns coordonat”[40]. Rusia consideră că activele EW ar putea dubla potențialul de luptă al forțelor terestre, reducând pierderile forțelor aeriene de șase ori și pierderile navale de trei ori 25, EW acționând astfel ca un instrument asimetric puternic. De asemenea, valoarea descurajantă a EW ar putea convinge inamicii să nu se angajeze în luptă împotriva Rusiei[41].

Ucraina a oferit un teren de probă pentru capacitățile EW dezvoltate de Rusia, iar zona de conflict sirian a fost descrisă drept „cel mai agresiv mediu EW de pe planetă” de

[36] (Doskalov 2013)
[37] (Doskalov 2013)
[38] (Kjellén 2018)
[39] (Kube 2018)
[40] (McDermott 2017)
[41] (Smith 2022)

către generalul Raymond Thomas, fostul comandant al Comandamentului Operațiunilor Speciale din Statele Unite[42]. O evaluare a lui Alan Shaffer, subsecretar adjunct pentru achiziții și susținere a apărării, susține că SUA „a pierdut spectrul electromagnetic”[43], iar William Conley, fost director al EW din SUA, a remarcat că s-a ajuns aici din cauza a „25 de ani de neatenție” și că „vom ieși din ea abia după 25 de ani de atenție.”[44]

Intenția Rusiei este să dețină o cotă mai mare din piața mondială a sistemelor militare EW. Dar industria rusă EW de astăzi se confruntă și cu o serie de provocări, precum atragerea tinerilor talentați, crearea clusterelor industriale EW, și embargoul ucrainean la export și sancțiunile occidentale[45].

NATO

NATO s-a concentrat tot mai mult pe războiul electronic, pe măsură ce tensiunile cu Rusia și preocupările cu privire la securitatea cibernetică cresc. Capacitățile EW sunt considerate cruciale pentru apărarea și securitatea țărilor membre, în special a celor care se învecinează cu Rusia. Abordarea NATO include îmbunătățirea capacităților sale defensive și ofensive EW, care implică bruiaj, interceptare și întreruperea comunicațiilor și radarului inamicului. Ei lucrează, de asemenea, la contracararea strategiilor anti-acces/denegare a zonei (A2/AD) care se bazează în mare măsură pe componente de război electronic.

NATO are o abordare cuprinzătoare a EW. În octombrie 1956, Comitetul militar a aprobat MC 0064, Politica NATO de război electronic. Alianța a dezvoltat ulterior Grupul de lucru NATO Electronic Warfare și apoi NATO Electronic Warfare L[46]. Un document din 2007, MCM_0142 Nov 2007 Military Committee Transformation Concept for Future NATO Electronic Warfare, a recunoscut EME ca spațiu/domeniu de manevră operațional și mediu/domeniu de luptă.

În perioada 25-27 noiembrie 2019, Comitetul Consultativ NATO pentru Războiul Electronic (NEWAC) a convocat cea de-a 107-a reuniune plenară la sediul NATO din Bruxelles. S-a discutat Strategia NATO EMS, recunoașterea EW ca disciplină de antrenament și îmbunătățirea politicii și conceptului NATO EW pentru viitorul EW.

[42] (Clark 2018)
[43] (Freedberg 2014)
[44] (Freedberg 2017)
[45] (Kjellén 2018)
[46] (NATO 2023)

Colonelul Kabasakal a subliniat importanța acestei strategii pentru NATO, „necesitatea ca forțele militare să aibă acces nestingherit și utilizarea mediului electromagnetic este esențială pentru succesul majorității operațiunilor militare. De asemenea, va determina eficiența contramăsurilor noastre în domeniul Războiului Electronic și capacitatea noastră de a ne proteja capacitățile și trupele”[47]. S-a dat ca exemplu Operațiunile Electromagnetice NATO (NEMO) desfășurate în octombrie.

NATO a adoptat un limbaj simplificat asemănător cu cel utilizat în alte medii de luptă (maritim, terestră, aerian/spațial), păstrând termenii tradiționali pentru contramăsuri electronice (ECM), măsuri electronice de protecție (EPM) și măsuri electronice de sprijin (ESM). Conform NATO, alte operațiuni EM includ informații, supraveghere, achiziție și recunoaștere ținte (ISTAR) și informații despre semnale (SIGINT).

Comitetul consultativ NATO pentru război electromagnetic (NEWAC), înființat în 1966, este principalul forum din cadrul NATO pentru consultarea și coordonarea aspectelor legate de EW. Acest comitet consiliază și aplică politicile Comitetului Militar, autoritatea militară superioară a NATO care consiliază Consiliul Nord-Atlantic. NEWAC este format din două grupuri de lucru: Grupul de lucru NATO privind războiul electromagnetic (NEWWG), și Grupul consultativ al bazelor de date ale emitenților NATO (NEDBAG) [48].

Statul Major de Război Electronic Comun al NATO(JEWCS) este o unitate militară multinațională pentru expertiză, sprijin și instruire în domeniul EW. Comitetul de legătură pentru războiul electronic (NEWLC) coordonează politica EW, echipamentele, cursurile de formare și publicațiile între Aliați[49].

NATO folosește acum termenul „război electromagnetic” pentru a identifica mai precis importanța spectrului electromagnetic în EW. Politica EW la NATO continuă să fie acoperită de MC 0064[50].

Uniunea Europeană

În timp ce UE în ansamblu nu este o alianță militară precum NATO, statele membre individuale au propriile lor capacități de război electronic și există eforturi la nivelul UE

[47] (NATO 2019)
[48] (NATO 2023)
[49] (NATO 2023)
[50] (NATO 2023)

pentru coordonarea în chestiuni de apărare, inclusiv EW. UE este preocupată în special de aspectul securității cibernetice a războiului electronic, având în vedere potențialele amenințări la adresa infrastructurii civile și a stabilității economice. Agenția Europeană de Apărare (EDA) sprijină dezvoltarea capacităților EW prin diferite proiecte de colaborare între statele membre, având ca scop îmbunătățirea bazei tehnologice colective și pregătirea operațională.

Planul de dezvoltare a capacităților (CDP) rămâne principala referință pentru planificatorii de apărare ai Uniunii Europene. „Securitatea viitoare a Europei depinde de un răspuns mai robust și mai agil. Lucrând împreună pentru a dezvolta capacități militare mai puternice și mai credibile, UE poate fi proactivă în a-și proteja securitatea, afirmându-și autonomia și asigurând siguranța și bunăstarea cetățenilor săi. Acest lucru va necesita un angajament profund față de colaborare și inovare, precum și o dorință de a adopta noile tehnologii", a afirmat Jin Sedivy, Director executiv EDA[51].

Conform CDP, o abordare bazată pe sisteme integrate colaborative multi-domeniu este considerată cea mai indicată strategie pentru a contracara amenințările emergente. Amenințările cibernetice și sistemele de război electronic sunt considerate cele mai mari amenințări, alături de utilizarea roiurilor de drone. Mediul electromagnetic se consideră că va ajunge mai congestionat, iar infrastructura aferentă va fi și mai critică din cauza creșterii uriașe a nevoilor de gestionare a datelor și comunicații. În consecință, libertatea de utilizare a spectrului electromagnetic va ajunge să fie o provocare, alături de mijloacele de război electronic, conștientizarea situației cibernetice și rezistența rețelelor. Operațiunile cu spectru electromagnetic (EMSO) vor avea un rol major, cu scopul de a obține dominația spectrului electromagnetic. Evoluțiile tehnologice care permit un avantaj față de adversar în spectrul electromagnetic vor fi esențiale, pentru a face față amenințărilor războiului electronic. Superioritatea cognitivă și tehnologiile de inteligență artificială pot îmbunătăți operațiunile în spectrul electromagnetic[52].

Pentru interceptarea armelor hipersonice și a atacurilor cu rachete balistice sunt necesare sisteme de apărare integrate și stratificate folosind sisteme non-cinetice, inclusiv

[51] (European Defence Agency 2023)
[52] (European Defence Agency 2023)

sistemele de război electronic, armele cu energie dirijată sau impulsurile electromagnetice, în special în atacurile de saturație[53].

În ceea ce privește Internetul obiectelor (IoT), principala preocupare se referă la securitatea cibernetică datorită vulnerabilităților la atacurile cibernetice, iar nevoia de rețele fără fir de mare capacitate va necesita o utilizare mai bine protejată a spectrului electromagnetic[54].

Sistemele autonome pot fi utilizate în sarcinile de război electronic pentru a proteja activele militare prin detectarea și neutralizarea amenințărilor din spectrul electromagnetic și pentru acțiuni ofensive, precum bruiajul.

Noile materiale și tehnici de fabricație (noi metale, biologie sintetică, nanotehnologie, design ascuns, etc.) vor influența capabilitățile avansate de comunicare în spectrul electromagnetic, iar antenele bazate pe metamateriale vor crește puterea de ieșire, vor îmbunătăți direcționalitatea și vor extinde gama de frecvență, făcându-le utile atât în războiul electronic ofensiv, cât și defensiv[55].

Conform Agenției Europene pentru Apărare,

> ”războiul electronic și mijloacele ofensive cibernetice vor juca un rol major în controlul spectrului electromagnetic puternic aglomerat al viitoarelor câmpuri de luptă, care va fi esențial pentru atingerea superiorității militare. Dezvoltarea de senzori mai buni și ieftini va îmbunătăți semnificativ sistemele de război electronic, care vor avea un efect puternic împotriva infrastructurilor critice, rețelelor de comunicații, platformelor și altor active critice. De asemenea, atacurile cibernetice vor fi folosite pentru a perturba sau degrada activele adversarilor de la distanță și chiar anonim, ceea ce va aduce mai multe posibilități și provocări pentru forțele militare. Robotica și sistemele autonome vor fi integrate pe scară largă în unitățile militare, îndeplinind o mare varietate de funcții în mai multe misiuni. Platformele autonome, formarea în echipă fără echipaj și adaptarea aferentă a tacticilor vor aduce mai multe provocări pentru protecția forței, dar vor prezenta și noi oportunități de a îndeplini misiuni cu mai puțin risc pentru viața umană. Îmbunătățirea umană ar putea fi, de asemenea, un factor perturbator pentru capacitățile de implicare. Evoluțiile tehnologice în domeniile exoscheletelor, senzorilor portabili, interfețele creier-calculator, sistemele bazate pe inteligență artificială, dispozitivele de realitate augmentată și virtuală (AR/VR) și dispozitivele de biologie sintetică vor permite îmbunătățiri semnificative ale abilităților fizice și cognitive ale soldaților.” [56]

[53] (European Defence Agency 2023)
[54] (European Defence Agency 2023)
[55] (European Defence Agency 2023)
[56] (European Defence Agency 2023)

Concluzie

Peisajul geopolitic care influențează războiul electronic implică o interacțiune complexă de descurajare, apărare și colectare de informații. Pe măsură ce tehnologia avansează, la fel crește și sofisticarea instrumentelor și tehnicilor de război electronic. Tensiunile în curs între aceste puteri în domeniile tehnologiei și securității subliniază importanța strategică a EW în conflictele militare actuale și viitoare.

Acest scenariu continuă să evolueze pe măsură ce fiecare entitate încearcă să-și îmbunătățească capacitățile și să se adapteze la mediul tehnologic în schimbare. Dezvoltarea și implementarea tehnologiilor EW sunt strâns legate de obiective strategice mai largi, care reflectă obiectivele și preocupările geopolitice ale fiecărei entități.

Urmărirea capabilităților avansate de război electronic a devenit o caracteristică definitorie a competiției militare contemporane, condusă de rivalitățile geopolitice, inovația tehnologică și imperativul modernizării militare. În timp ce războiul electronic oferă avantaje strategice și superioritate operațională, el ridică și provocări cu mai multe fațete legate de proliferare, etică și vulnerabilități cibernetice. Navigarea prin complexitățile competiției internaționale în războiul electronic avansat necesită o înțelegere nuanțată a implicațiilor sale pentru securitatea națională, stabilitate și dinamica evolutivă a războiului modern.

Competiția internațională în războiul electronic avansat modifică strategiile militare și afectează securitatea globală. Pe măsură ce națiunile investesc masiv în dezvoltarea de capabilități sofisticate de EW, potențialul de conflict crește, necesitând o cooperare și o reglementare internațională robustă. Încurajând dialogul și stabilind norme pentru operațiunile EW, comunitatea internațională poate contribui la asigurarea faptului că aceste tehnologii puternice sunt utilizate în mod responsabil și nu conduc la o creștere a instabilității globale. Viitorul securității internaționale va depinde în mod semnificativ de modul în care națiunile gestionează provocările generate de războiul electronic avansat.

Bibliografie

* * *. 1984. *Voennyi Entsiklopedicheskii Slovar*. Moscova: Voennoe Izadatelstvo.
———. 1990. *Voenno-morskoi Slovar*. Moscova: Voennoe Izadatelstvo.

Allen, Gregory C. 2019. *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security*. Center for a New American Security.

Army, United States Government US. 2020. *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.

Baker, James E. 2018. „Artificial intelligence and national security law: A dangerous nonchalance | MIT Center for International Studies". 2018. https://cis.mit.edu/publications/starr-forum-report/18-01-report.

Carlin, John P. 2016. „Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats | CSIS Events". 2016. https://www.csis.org/events/detect-disrupt-deter-whole-government-approach-national-security-cyber-threats.

Clark, Colin. 2018. „Russia Widens EW War, «Disabling» EC-130s OR AC-130s In Syria". *Breaking Defense* (blog). 24 aprilie 2018. https://breakingdefense.sites.breakingmedia.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.

Copp, Tara. 2021. „'It Failed Miserably': After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight". Defense One. 26 iulie 2021. https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/.

CRS. 2022. „Defense Primer: Electronic Warfare". https://sgp.fas.org/crs/natsec/IF11118.pdf.

DoD. 2022. „DoD Announces Release of JADC2 Implementation Plan". U.S. Department of Defense. 2022. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F2970094%2Fdod-announces-release-of-jadc2-implementation-plan%2F.

Doskalov, Mikhail. 2013. „Perspektivy razvitiia sistemy radioelektronnoi borby Rossiiskoj Federatsii na period do 2020 goda". În *Oboronnyi kompleks RF: Sostoianie i razvitie*. http://federalbook.ru/files/OPK/Soderjanie/OPK-9/III/Doskalov.pdf.

Duke, Audrey. 2023. „Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations". https://apps.dtic.mil/sti/citations/AD1206172.

European Defence Agency. 2023. „Enhancing EU Military Capabilities Beyond 2040". https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf.

Freedberg, Sydney J. 2014. „US Has Lost «Dominance In Electromagnetic Spectrum»: Shaffer". *Breaking Defense* (blog). 3 septembrie 2014. https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/.

———. 2017. „Electronic Warfare «Growing»; Joint Airborne EW Study Underway". *Breaking Defense* (blog). 23 iunie 2017. https://breakingdefense.sites.breakingmedia.com/2017/06/electronic-warfare-growing-joint-airborne-ew-study-underway/.

Friedrich, Nancy. 2020. „AI and Machine Learning Redefine the EW Landscape | 2020-12-08 | Microwave Journal". 2020. https://www.microwavejournal.com/articles/35107-ai-and-machine-learning-redefine-the-ew-landscape.

Guzenko, V. F., și A. L. Moraresku. 2017. *Radioelektronnaia borba. Sovremennoe soderzhanie*. Moscova: Informatsionnyi Most.

Haney, Brian. 2019. „Applied Artificial Intelligence in Modern Warfare and National Security Policy". SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3454204.

Henney, Megan. 2019. „Big Tech Has Spent $582M Lobbying Congress. Here's Where That Money Went". Text.Article. FOXBusiness. Fox Business. 8 mai 2019. https://www.foxbusiness.com/technology/amazon-apple-facebook-google-microsoft-lobbying-congress.

Hoehn, John. 2021. „Defense Primer: What Is Command and Control?" https://apps.dtic.mil/sti/citations/AD1169627.

Insinna, Valerie. 2022. „China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates". *Breaking Defense* (blog). 29 noiembrie 2022. https://breakingdefense.sites.breakingmedia.com/2022/11/china-to-obtain-1500-nuclear-warheads-by-2035-pentagon-estimates/.

Kjellén, Jonas. 2018. „Russian Electronic Warfare - The role of Electronic Warfare in the Russian Armed Forces". https://web.archive.org/web/20181010174505/https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C4c547bec-bdfa-4bdb-a1c9-018097aaf615.pdf.

Kolesov, N. A., și I. G. Nasenkov. 2015. *Radioelektronnaia Borba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego*. Moscova: Centre for Analysis of Strategies and Technologies (CAST).

Kolhatkar, Sheelah. 2019. „How Elizabeth Warren Came Up with a Plan to Break Up Big Tech". *The New Yorker*, 20 august 2019. https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech.

Krylov, G. O., S. L. Larionova, și Nikitina. 2017. *Bazovye poniatiia informatsionnoi bezopasnosti*. Moscova: OOO RUSAJNS.

Kube, Courtney. 2018. „Russia Is Jamming American Drones in Syria, Officials Say". NBC News. 10 aprilie 2018. https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

Lakhin, Andrei, și Andrei Korobeinikov. 2016. *Sostoianie i perspektivy razvitiia voisk radioelektronnoi borby Vooruzhennykh Sil Rossiiskoi Federatsii*. Moscova: Informatsionnyi Most.

Liubin, Mikhail Dmitriyevich. 2009. „K voprosu ob istorii razvitiia i perspektivakh radioelektronnoi borby". *Voennaia mysl*, nr. 3: 64–75.

McDermott, Roger N. 2017. „Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum". ICDS. 17 septembrie 2017. https://icds.ee/en/russias-electronic-warfare-capabilities-to-2025-challenging-nato-in-the-electromagnetic-spectrum/.

NATO. 2019. „The 107th NATO Electronic Warfare Advisory Committee (NEWAC) Convenes in Brussels". NATO. 2019. https://www.nato.int/cps/en/natohq/news_171280.htm.

———. 2023. „Electromagnetic Warfare". NATO. 2023. https://www.nato.int/cps/en/natohq/topics_80906.htm.

Northrop. 2022. „Electronic Warfare and Sensors". https://info.breakingdefense.com/hubfs/E-Book_EW_&_Sensors_Northrop_Grumman_Breaking_Defense.pdf.

ODIN. 2023. „Borisoglebsk-2 (RB-301B) Russian Amphibious Multipurpose Jamming Complex". 2023. https://odin.tradoc.army.mil/WEG/Asset/Borisoglebsk-2_(RB-301B)_Russian_Amphibious_Multipurpose_Jamming_Complex.

Rogosa, Alexander. 2015. „Shifting Spaces: The Success of the SpaceX Lawsuit and the Danger of Single-Source Contracts in America's Space Program". *Federal Circuit Bar Journal* 25: 101.

Smith, Patrick. 2022. *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project.

You, Shixun, Ming Diao, și Lipeng Gao. 2019. „Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare". *IEEE Access* 7: 37432–47. https://doi.org/10.1109/ACCESS.2019.2905649.